



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/581,459	07/27/2000	STEPHAN SCHMITZ	10191/1452	7359
26646	7590	12/15/2006	EXAMINER	
KENYON & KENYON LLP ONE BROADWAY NEW YORK, NY 10004			LIPMAN, JACOB	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 12/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

DEC 15 2006

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/581,459
Filing Date: July 27, 2000
Appellant(s): SCHMITZ ET AL.

Gerald A. Messina
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 14 September 2006 appealing from the Office action mailed 14 April 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,745,576	Abraham et al.	4-1998
4,797,672	Kousa	1-1989
6,070,243	See et al.	5-2000

Schneier, Applied Cryptography, 1996, John Wiley and Sons Inc., Second edition, pages 47-51, 179, and 180

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 10, 11, and 14-18 are rejected under 35 U.S.C. 103(a) as being anticipated by Abraham et al., US Patent number 5,745,576 in view of Kousa, US Patent number 4,797,672.

With regard to claim 10, Abraham discloses a base station (controller) including a computer (column 12 lines 13-47) that transmits a prompt (column 9 lines 56-61, column 10 lines 56-59), and a remote control device (terminal, column 1 lines 13-15) which stores the prompt (column 9 lines 21-24, column 10 lines 60-62), and transmits a code word as a reply (column 9 lines 24-30, column 10 lines 63-64) that is partially a function of the prompt (column 9 lines 24-26, column 10 lines 64-65), the base station receives the reply and compares it with the required reply (column 10 lines 66-67), and grants access accordingly (column 11 lines 1-3). Abraham does not disclose that an initial stored prompt from a successful prompt/reply cycle is used to encrypt the authorization information. Kousa discloses that often an encrypted exchange will be preceded by a key exchange to create a session key to use in further authentications (column 2 lines 3-10). It is further added that the examiner takes official notice that key exchange to begin a session is well known in the art. It would have been obvious for

Art Unit: 2134

one of ordinary skill in the art to use key exchange preceding Abraham to prevent eavesdropping. With regard to the base computer erasing the session key after a number of failed attempts, Abraham does not mention abandoning the process after a specific number of failed attempts. The examiner takes official notice that it is well known in the art to check failed attempts to connect, and to abandon an access process after a predetermined number of failures. It would have been obvious for one of ordinary skill in the art to use this check in Abraham's system to avoid eternal loops, and to increase security against hacking. Support for this can be seen in See et al., USPN 6,070,243. See discloses terminating a session with a user after a predetermined number of failed login attempts (column 11 lines 15-38). Further Schneier discloses that session keys are erased when a session is ended (page 180, paragraph beginning "some").

With regard to claim 11, Abraham discloses the response is a function of the terminal's serial number (column 9 lines 24-28).

With regard to claim 12, Abraham discloses the challenge is stored in the base system (column 9 lines 56-59).

With regard to claim 14, Abraham discloses the reply includes a transaction count (column 9 lines 24-26), which is tracked (column 10 lines 22-24).

With regard to claim 15, Abraham discloses the count is changed (column 31-35).

With regard to claim 16, Abraham discloses the counter code has been previously transmitted to the base station (column 9 lines 42-46).

With regard to claim 17, Abraham discloses the counter code is encrypted (column 9 lines 24-26).

With regard to claim 18, Abraham discloses the system of claim 10, as outlined above, but does not mention wireless communication or frequencies. The examiner takes official notice that it is well known in the art to have different wireless device working on different frequencies. It would have been obvious for one of ordinary skill in the art to use Abraham's system in a wireless environment with different frequencies to avoid interference and allow mobility.

(10) Response to Argument

With regard to applicant's argument that, "the encrypted challenge message must be stored to be decrypted" is nothing more than a self-serving statement, the examiner disagrees. It is well known in the art, that a computer cannot take action on data without storing it somewhere first. Further, Abraham discloses storing an initial key and hashing it to get the next key, which is also stored (column 7 lines 10-20).

With regard to applicant's argument that Abraham does not teach a system for access authorization, the examiner points out that this has never been claimed. The claims state "A system for controlling an access authorization". Abraham authenticates a cryptographic terminal so that the terminal can be accessed, and it can access other data. This can be seen in column 6 line 27-column 7 line 9. Further, Fig 3 has a final step of the controller welcoming the terminal.

The applicant argues that there is no motivation to combine Abraham and Kousa. The examiner points out that Abraham discloses a system that includes an initial key

using a stored value (count value) to create an encryption key (column 4 lines 12-20). While the count value is from a former prompt reply/cycle, it is not necessarily from an initial prompt/reply cycle. While Abraham discloses information being sent a received, he does not disclose a specific wrapper to secure information from attacks and eavesdropping. Kousa discloses that often an encrypted exchange will be preceded by a key exchange to create a session key to use in further authentications (column 2 lines 3-10), and could thus prevent eavesdropping and other attacks that are very well known in the art (column 1 lines 52-58).

With regard to applicant's argument that the examiner has failed to show that it would be obvious to delete the initial prompt after a predetermined number of failed attempts, the examiner points again to See and Schneier. It is very well known in the art to allow only a predetermined number of access attempts before refusing further attempts, as shown in See. In the combination of Abraham and Kousa, it would not be practical to hold onto the negotiated initial key, without overloading memory with extra useless keys. That is why it would be obvious to one of ordinary skill in the art to apply the teaching of Schneier to delete a session key when the session is over.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Art Unit: 2134

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Jacob Lipman



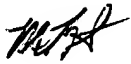
Conferees:

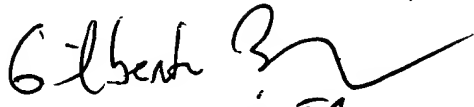


Gilberto Barron



Matthew Smithers




GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100